

普通高等学校网络工程专业规划教材

丛书总主编：杨云江

# 网络安全技术

曾湘黔 主编

清华大学出版社



普通高等学校网络工程专业规划教材

丛书总主编：杨云江

# 网络安全技术

曾湘黔 主编

任新 曾劼 刘毅 编著

清华大学出版社

北京

## 内 容 简 介

本书全面系统地介绍了计算机网络安全技术。全书共分 13 章,内容包括网络安全概述、密码学与信息安全、网络安全协议、网络设备常见安全技术、Internet 安全技术、网络操作系统安全分析及防护、防火墙技术、入侵检测技术、网络嗅探技术、端口扫描技术与漏洞扫描技术、网络病毒防范技术、黑客攻击与防护技术、网络安全解决方案。

本书每章都有思考题,有针对性地帮助读者理解本书的内容。

本书可作为高校计算机及其相关专业“网络安全技术课程”教材,也可供相关的技术人员使用。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

### 图书在版编目(CIP)数据

网络安全技术/曾湘黔主编. —北京:清华大学出版社,2013.1

普通高等学校网络工程专业规划教材

ISBN 978-7-302-29391-0

I. ①网… II. ①曾… III. ①计算机网络—安全技术—高等学校—教材 IV. ①TP393.08

中国版本图书馆 CIP 数据核字(2012)第 159738 号

责任编辑:袁勤勇 顾 冰

封面设计:康瑞学

责任校对:时翠兰

责任印制:何 芊

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦 A 座 邮 编:100084

社 总 机:010-62770175 邮 购:010-62786544

投稿与读者服务:010-62776969, [c-service@tup.tsinghua.edu.cn](mailto:c-service@tup.tsinghua.edu.cn)

质量反馈:010-62772015, [zhiliang@tup.tsinghua.edu.cn](mailto:zhiliang@tup.tsinghua.edu.cn)

课件下载: <http://www.tup.com.cn>, 010-62795954

印 装 者:北京鑫海金澳胶印有限公司

经 销:全国新华书店

开 本:185mm×260mm 印 张:22.5

字 数:549 千字

版 次:2013 年 1 月第 1 版

印 次:2013 年 1 月第 1 次印刷

印 数:1~3000

定 价:34.50 元

# 普通高等学校网络工程专业规划教材

## 编审委员会

**编委会名誉主任：**谢晓尧 贵州省政协副主席、教授、博士生导师

曾羽 贵州理工学院党委书记、教授

李祥 贵州大学名誉校长、教授、博士生导师

**编委会主任：**杨云江 贵州大学信息化管理中心 教授、硕士生导师

**编委(按姓名汉语拼音字母顺序排列)：**

陈梅 贵州大学计算机学院副院长、副教授、硕士生导师

陈文举 贵州大学职业技术学院院长、教授

陈芙蓉 贵州大学计算机学院副院长、教授、硕士生导师

邓洁 贵州大学科技学院副院长、副教授

刘志杰 贵州师范大学网络中心主任、教授、博士

彭长根 贵州大学理学院教授、博士、硕士生导师

索洪敏 贵州民族学院计算机学院副院长、教授

汪学明 贵州大学计算机学院教授、硕士生导师、博士

王子牛 贵州大学信息化管理中心副主任、副教授、硕士生导师

文静华 贵州财经学院信息学院副院长、教授

杨健 贵州大学信息化管理中心副主任、副教授、博士、硕士生导师

殷英 贵州大学教务处副处长、副教授

曾湘黔 贵州大学职业技术学院副院长、副教授

张仁津 贵州师范大学数学与计算机科学学院副院长、教授、硕士生导师

## 丛书序

当今的世界,是计算机网络的时代,也是信息的时代,计算机网络已成为人们获取信息和交流信息的一种重要手段,它正深刻影响着人类社会的发展及经济运行模式,影响着人们的工作、学习和生活方式。为此,社会的各行各业都投入了大量的人力和物力建设与实施基于计算机网络的信息化工程,因此,迫切需要大量掌握计算机网络系统规划、设计、建设、运行、管理和维护的实用型网络技术的高级人才,网络工程专业正是为顺应这种社会需求而诞生的新兴专业。

网络工程专业是面向网络工程应用的计算机科学与技术类专业,旨在培养具有计算机网络基础知识和抽象思维能力,掌握计算机网络软硬件基本理论和技术,掌握网络工程的基本原理与实现方法,能运用所学的知识与技能去分析和解决网络工程的实际问题。由于网络工程专业毕业生更容易成为从事计算机网络的建设和应用、计算机网络的管理与维护、网络工程的开发与集成等方面的高层次网络人才,深受社会各界的广泛关注和青睐,近几年来该专业的毕业生就业率都居高不下。

自2001年经教育部批准,同意11所高校开办本科网络工程专业以来,每年都有数十所高等院校申请开设网络工程专业。截止2010年6月,开设网络工程专业的高校已达260所。这表明,网络工程专业在我国高等教育中越来越受到重视。

在这种形势下,作为普通高校,如何适应时代的需求,培养掌握计算机网络及其相关技术的高素质网络工程人才,以满足不同行业不同岗位对网络工程人才的需求,成为一项既紧迫又重要的战略任务。为达到此目标,高校除了需要具有良好的教学环境、先进的教学设施和优秀的师资队伍之外,更重要的是需要一套符合现代网络工程专业需求的高校教材。

多年来,全国各出版社出版了大量的计算机技术类及信息技术类的高校教材,这些教材为我国高等教育事业作出了巨大的贡献。但是,这些教材很多都是理论性太强,弱化了实用性,特别是很少涉及网络工程设计与建设、网络工程实践与管理等方面的内容。因此,上述传统的教材大多数已不再适应当代网络

# F O R E W O R D

工程专业的教学需求。为了培养出符合现代社会需求的实用型网络工程的技术人才,必须对传统的教学模式和教材进行改革。在清华大学出版社的鼎力支持下,本套丛书的编委会及作者根据网络工程专业的特点和需求,在广泛征求意见和充分酝酿的基础上,组织编写了这套满足普通高校本科网络工程专业需求的教材。

本套丛书最显著的特色是:理论与实践相结合、强调网络工程专业的特点、突出实用性和可操作性、注重实践技能的训练,提高学生的创新能力,以达到培养实用型的网络工程技术人才的目的。

丛书的主要编写模式是:教材紧紧围绕网络工程应用进行构思和编写,在介绍相关理论知识的基础上,给出大量的应用实例,并有完整的实用案例分析。在教材中,将实用案例作为一个工程项目来看待,强调从工程项目的角度出发,在进行需求分析的基础上,给出案例的详细设计与实施步骤,旨在帮助学生在学完每一门课程后,将所学的知识运用到应用程序的设计与开发,应用到网络工程的规划与设计、建设与管理之中。

本书主编及参编者都是长期从事计算机科学及网络技术的教学工作、网络工程建设与管理工作的高校教师,具有较深的理论知识、丰富的教学经验和网络管理经验。本套丛书是这些教师多年教学、网络开发与应用、网络管理与维护经验和心得体会的结晶。

为了保证本套教材的编写质量,我们组织了由高校专家、学者组成的教材编审委员会,编委会负责对教材的结构及书稿内容进行全程的指导和监督,并负责对书稿内容进行审查。

很高兴能看到本套丛书的出版,希望本套丛书能为我国高等教育贡献微薄之力,更希望本套丛书能给广大师生和读者带来收益和帮助。

贵州省政协副主席、博士生导师 谢晓尧  
丛书编委会名誉主任  
2011年5月18日



## 前 言

计算机网络的出现及发展,给人们的工作和生活都带来了极大的方便。随着人们对计算机网络的依赖程度的增加,越来越多的信息和重要数据资源出现在网络中,一旦网络由于种种原因发生故障,陷于瘫痪,人们的生活必然受到极大的影响。另外,计算机犯罪的日益增多也对网络的安全运行和发展提出了挑战,如何保障计算机安全及网络安全已成为目前一个亟待解决的问题。因此,网络安全技术成为当前网络技术的重要研究课题和发展方向。

本书紧密结合计算机网络安全技术的最新发展,系统地介绍了计算机网络安全的基础理论、技术原理和相关案例,使读者对计算机网络安全有一个系统、全面的了解。本书共 13 章,第 1 章主要介绍网络安全的特征、网络面临的安全威胁、网络安全体系结构、网络安全评价标准。第 2 章主要介绍数据加密标准、RSA 公钥密码体制、MD5、身份认证技术、数字取证技术。第 3 章主要介绍 SSL 协议、SSH 协议、SET 协议、IPSec 协议。第 4 章主要介绍交换机原理及 VLAN 原理、加密技术、身份认证技术原理、VPN 技术原理、无线网络安全技术原理。第 5 章主要介绍网络操作系统安全、TCP/IP 协议安全、电子邮件安全漏洞及防范、Telnet 安全漏洞及防范、FTP 安全漏洞及防范、Web 服务器安全漏洞及防范、拒绝服务攻击原理及防范、缓冲区溢出攻击及防范、DNS 欺骗与防范技术、IP 地址欺骗、盗用及防范技术。第 6 章主要介绍网络操作系统常见漏洞、Windows 2003/XP 操作系统的漏洞分析与防范、UNIX 操作系统漏洞分析与防范、Windows 2003 漏洞扫描工具 MBSA 的使用、UNIX 常用漏洞扫描工具 Nessus 的使用、在 Windows 2003 上搭建安全的 FTP 和 Web 服务器、UNIX 上搭建安全的 FTP 和 Web 服务器。第 7 章主要介绍防火墙的功能与分类、防火墙的主要技术、防火墙体系结构、防火墙配置、防火墙的选型、主流防火墙产品、防火墙发展动态与趋势、防火墙部署实例。第 8 章主要介绍入侵检测概述、入侵检测技术、入侵检测系统的标准、入侵检测系统部署、典型入侵检测产品。第 9 章主要介绍网络嗅探监听的原理、网络监听的防范措施、典型嗅探监听工具。第 10 章主要介绍端口扫描技术、漏洞扫描技术、典型的端口扫描与漏洞扫描产品。第 11 章主要介绍网络病毒基础、病毒检测与防范技术、典型



# P R E F A C E

病毒检测与防范产品、网络病毒防范实例。第12章主要介绍黑客基本概念、黑客攻击及防范技术、应用实例。第13章主要介绍网络安全解决方案设计、网络安全解决方案实例。

本书由曾湘黔担任主编并负责统稿,第10~13章由曾湘黔编写,第1~3章由任新编写;第4~6章由刘毅编写;第7~9章由曾劼编写。杨云江教授担任丛书编审委员会主任兼丛书总主编,负责全书目录结构、书稿内容结构的组织、规划与审定以及书稿的初审工作。

由于作者水平有限,书中难免有不足之处,望读者批评指正。

编者

2012年5月



## 目 录

<b>第 1 章 网络安全概述</b> .....	1
1.1 网络安全的概念与特征 .....	1
1.1.1 网络安全的概念 .....	1
1.1.2 网络安全的特征 .....	2
1.2 网络面临的安全威胁 .....	2
1.2.1 网络安全现状 .....	2
1.2.2 安全威胁分析 .....	3
1.3 网络安全体系结构 .....	4
1.3.1 网络安全模型 .....	4
1.3.2 OSI 安全体系结构 .....	5
1.3.3 P2DR 模型 .....	11
1.4 网络安全管理 .....	13
1.4.1 网络安全管理的法律法规 .....	13
1.4.2 网络安全评价标准 .....	15
思考题 .....	17
<b>第 2 章 密码学与信息安全</b> .....	18
2.1 密码学基础 .....	18
2.1.1 基本概念 .....	18
2.1.2 对称密码与非对称密码体制 .....	19
2.1.3 密码分析的攻击类型 .....	19
2.1.4 经典密码学 .....	20
2.2 对称密码体制 .....	23
2.2.1 基本概念 .....	23
2.2.2 数据加密标准 .....	23
2.2.3 加密算法 .....	24

# C O N T E N T S

2.2.4 密钥交换技术 .....	29
2.3 非对称(公钥)密码 .....	29
2.3.1 基本思想 .....	29
2.3.2 RSA 公钥密码体制 .....	30
2.3.3 对称与非对称密钥加密 .....	32
2.4 认证理论与技术 .....	33
2.4.1 单向 Hash 函数 .....	33
2.4.2 MD5 算法 .....	34
2.5 身份认证技术 .....	38
2.6 数字取证技术 .....	40
2.7 密码学综合应用实例 .....	42
2.7.1 数字签名技术 .....	42
2.7.2 数字信封技术 .....	46
2.7.3 密钥管理技术 .....	48
2.7.4 消息完整性检验技术 .....	49
思考题 .....	50
<b>第3章 网络安全协议 .....</b>	<b>52</b>
3.1 SSL 协议 .....	52
3.1.1 SSL 概述 .....	52
3.1.2 SSL 体系结构与协议 .....	53
3.1.3 SSL 安全性分析 .....	56
3.1.4 SSL 协议的应用 .....	57
3.2 TLS 协议 .....	58
3.2.1 TLS 概述 .....	58
3.2.2 TLS 协议结构 .....	58
3.2.3 TLS 记录协议 .....	59
3.2.4 TLS 握手协议 .....	61
3.2.5 TLS 安全性分析 .....	62
3.3 SSH 协议 .....	63
3.3.1 SSH 概述 .....	63

# C O N T E N T S

3.3.2	SSH 协议体系结构 .....	64
3.3.3	SSH 传输协议 .....	65
3.3.4	SSH 身份认证协议 .....	66
3.3.5	SSH 连接协议 .....	67
3.3.6	SSH 协议的应用 .....	67
3.3.7	SSH 安全性分析 .....	68
3.4	SET 协议 .....	69
3.4.1	SET 协议概述 .....	69
3.4.2	SET 协议基本流程 .....	71
3.4.3	SSL 和 SET 协议比较 .....	72
3.4.4	SET 协议安全性分析 .....	72
3.5	IPSec 协议 .....	73
3.5.1	IPSec 体系结构 .....	73
3.5.2	验证文件头协议 AH .....	74
3.5.3	IPSec 安全协议 ESP .....	76
3.5.4	Internet 安全关联密钥管理协议 .....	79
3.6	QoS 协议 .....	82
3.6.1	QoS 的体系结构 .....	82
3.6.2	QoS 的实现机制 .....	83
	思考题 .....	85
<b>第 4 章</b>	<b>网络设备常见安全技术 .....</b>	<b>86</b>
4.1	局域网络安全技术 .....	86
4.1.1	网络分段 .....	86
4.1.2	以交换式集线器代替共享式集线器 .....	87
4.1.3	VLAN 的划分 .....	88
4.2	广域网络安全技术 .....	90
4.2.1	加密技术 .....	90
4.2.2	VPN 技术 .....	91
4.2.3	身份认证技术 .....	92
4.3	VPN 技术 .....	93
4.3.1	隧道技术 .....	93

# C O N T E N T S

4.3.2	加密技术	97
4.3.3	访问控制技术	98
4.4	无线网络安全技术	99
4.4.1	隐藏 SSID	99
4.4.2	MAC 地址过滤	100
4.4.3	WEP 加密	101
4.4.4	WPA	103
4.4.5	WPA2	106
4.4.6	IEEE 802.11i	107
4.4.7	AP 隔离	107
4.4.8	IEEE 802.1x 协议	109
	思考题	111
<b>第 5 章</b>	<b>Internet 安全技术</b>	<b>112</b>
5.1	Internet 存在的安全漏洞	112
5.1.1	Internet 网络安全概述	112
5.1.2	网络操作系统安全漏洞	115
5.1.3	Internet 应用安全漏洞	116
5.2	TCP/IP 安全性分析	117
5.2.1	TCP 协议工作过程及安全问题	117
5.2.2	IP 协议安全问题	121
5.2.3	ICMP 协议的安全问题	122
5.3	Web 安全与 HTTP 访问安全技术	124
5.3.1	Web 服务器上的漏洞	124
5.3.2	如何在 Web 上提高系统安全性和稳定性	127
5.3.3	HTTP 访问安全	129
5.4	电子邮件安全技术	130
5.4.1	电子邮件面临的安全问题	130
5.4.2	电子邮件的安全措施	131
5.5	Telnet 安全技术	132
5.5.1	Telnet 安全性分析	132

# C O N T E N T S

5.5.2	保障 Telnet 安全的策略分析 .....	134
5.5.3	安全的 Telnet 系统介绍 .....	134
5.6	FTP 安全技术 .....	136
5.6.1	FTP 工作原理与工作方式 .....	136
5.6.2	FTP 服务器软件漏洞 .....	137
5.6.3	安全策略 .....	139
5.7	DNS 欺骗与防范技术 .....	140
5.7.1	DNS 欺骗原理 .....	140
5.7.2	防范 DNS 欺骗攻击方法 .....	142
5.8	IP 地址欺骗与防范技术 .....	145
5.8.1	IP 地址欺骗原理 .....	145
5.8.2	IP 欺骗的防范措施 .....	147
5.9	IP 地址盗用与防范技术 .....	148
5.9.1	IP 地址盗用的常用方法 .....	148
5.9.2	IP 地址盗用防范技术 .....	149
5.10	缓冲区溢出攻击与防范技术 .....	150
5.10.1	缓冲区溢出漏洞的产生原因 .....	151
5.10.2	缓冲区溢出漏洞的危害性 .....	153
5.10.3	防范及检测方法 .....	154
5.11	拒绝服务攻击与防范技术 .....	155
5.11.1	拒绝服务攻击基本概念 .....	156
5.11.2	攻击原理 .....	156
5.11.3	抵御攻击的技术手段 .....	157
	思考题 .....	161
<b>第 6 章</b>	<b>网络操作系统安全分析及防护 .....</b>	<b>162</b>
6.1	网络操作系统安全概述 .....	162
6.1.1	网络操作系统安全问题 .....	162
6.1.2	网络操作系统安全控制 .....	165
6.2	Windows 2003/XP 操作系统安全分析与防护 .....	167
6.2.1	Windows 2003/XP 安全机制 .....	167

# C O N T E N T S

6.2.2	Windows 2003/XP 漏洞分析 .....	169
6.2.3	Windows 2003/XP 安全策略 .....	171
6.2.4	Windows 2003/XP 安全防护 .....	173
6.3	UNIX 安全性及防护 .....	178
6.3.1	UNIX 系统简介 .....	178
6.3.2	UNIX 系统的安全机制 .....	180
6.3.3	UNIX 安全漏洞 .....	182
6.3.4	UNIX 安全策略 .....	184
6.3.5	UNIX 安全防护 .....	186
6.4	操作系统安全应用实例 .....	187
6.4.1	Windows 系统漏洞的检测与修补 .....	187
6.4.2	Windows 中 Web、FTP 服务器的安全配置 .....	192
6.4.3	UNIX 系统漏洞的检测与修补 .....	201
6.4.4	UNIX 中 Web、FTP 服务器的安全配置 .....	212
	思考题 .....	218
<b>第 7 章</b>	<b>防火墙技术 .....</b>	<b>219</b>
7.1	防火墙基础 .....	219
7.1.1	防火墙的定义 .....	219
7.1.2	防火墙的特点 .....	219
7.2	防火墙的功能与分类 .....	220
7.2.1	防火墙的功能 .....	220
7.2.2	防火墙的分类 .....	220
7.3	防火墙的主要技术 .....	221
7.3.1	包过滤技术 .....	221
7.3.2	应用级网关防火墙 .....	222
7.3.3	深度包过滤技术 .....	223
7.4	防火墙体系结构 .....	226
7.5	防火墙配置 .....	227
7.5.1	网络防火墙配置 .....	227
7.5.2	防火墙的组网结构 .....	228

# C O N T E N T S

7.5.3	个人防火墙配置 .....	230
7.6	防火墙的选型 .....	234
7.6.1	防火墙的选择原则 .....	234
7.6.2	选择防火墙的两个要素 .....	234
7.7	主流防火墙产品简介 .....	235
7.7.1	天融信防火墙 .....	235
7.7.2	联想防火墙 .....	235
7.7.3	瑞星防火墙 .....	237
7.7.4	360 ARP 防火墙 .....	237
7.8	防火墙发展动态与趋势 .....	238
7.9	防火墙部署实例 .....	241
7.9.1	某校园网防火墙部署 .....	241
7.9.2	某公司网络防火墙部署 .....	242
7.9.3	某餐饮企业防火墙方案 .....	243
	思考题 .....	244
<b>第 8 章</b>	<b>入侵检测技术 .....</b>	<b>245</b>
8.1	入侵检测概述 .....	245
8.1.1	入侵检测原理 .....	246
8.1.2	入侵检测系统结构 .....	247
8.1.3	入侵检测系统分类 .....	249
8.2	入侵检测技术 .....	252
8.2.1	入侵检测分析模型 .....	252
8.2.2	误用检测 .....	253
8.2.3	异常检测 .....	254
8.2.4	其他检测技术 .....	255
8.3	入侵检测系统的标准 .....	255
8.3.1	IETF/IDWG .....	255
8.3.2	CIDF .....	257
8.4	入侵检测系统部署 .....	259
8.4.1	入侵检测系统部署的原则 .....	259



# C O N T E N T S

8.4.2	入侵检测系统部署实例 .....	259
8.4.3	入侵检测特征库的建立与应用 .....	261
8.5	典型入侵检测产品简介 .....	265
8.5.1	入侵检测工具 Snort .....	265
8.5.2	Cisco 公司的 NetRanger .....	265
8.5.3	Network Associates 公司的 CyberCop .....	266
8.5.4	Internet Security System 公司的 RealSecure .....	266
8.5.5	中科网威的“天眼”入侵检测系统 .....	267
8.6	案例——Snort 的安装与使用 .....	267
	思考题 .....	269
<b>第 9 章</b>	<b>网络嗅探技术 .....</b>	<b>270</b>
9.1	网络嗅探监听原理 .....	270
9.1.1	网卡工作原理 .....	270
9.1.2	网络嗅探监听原理 .....	271
9.1.3	网络嗅探器接入方案 .....	272
9.1.4	无线局域网嗅探技术原理 .....	273
9.2	网络监听的防范措施 .....	274
9.2.1	局域网网络监听的防范措施 .....	274
9.2.2	无线局域网网络监听的防范措施 .....	276
9.3	典型嗅探监听工具 .....	277
9.3.1	Tcpdump/Windump .....	277
9.3.2	Sniffit .....	280
9.3.3	Ettercap .....	282
9.3.4	Snarp .....	289
	思考题 .....	290
<b>第 10 章</b>	<b>端口扫描技术与漏洞扫描技术 .....</b>	<b>291</b>
10.1	端口扫描技术 .....	291
10.1.1	TCP connect() 扫描 .....	291
10.1.2	半连接扫描 .....	291
10.1.3	TCP FIN 扫描 .....	292

# C O N T E N T S

10.2	漏洞扫描技术 .....	292
10.2.1	漏洞扫描概述 .....	292
10.2.2	漏洞扫描技术的原理 .....	293
10.2.3	漏洞扫描技术的分类和实现方法 .....	293
10.3	典型的端口扫描与漏洞扫描产品简介 .....	294
10.3.1	Nmap 端口扫描工具 .....	294
10.3.2	ScanPort 端口扫描工具 .....	297
10.3.3	安铁诺防病毒软件漏洞扫描工具 .....	297
10.3.4	NeWT Security Scanner v1.0 网络漏洞扫描工具 ..	297
	思考题 .....	297
<b>第 11 章</b>	<b>网络病毒防范技术</b> .....	<b>298</b>
11.1	网络病毒基础 .....	298
11.1.1	计算机病毒的概念 .....	298
11.1.2	计算机病毒的特征 .....	298
11.1.3	计算机病毒的结构 .....	299
11.1.4	网络病毒的特征与传播方式 .....	300
11.2	病毒检测与防范技术 .....	300
11.2.1	病毒检测技术 .....	300
11.2.2	病毒防范技术 .....	302
11.3	典型病毒检测与防范产品简介 .....	304
11.4	网络病毒防范实例 .....	305
11.4.1	病毒特征码的提取及应用技术 .....	305
11.4.2	宏病毒及防范 .....	306
11.4.3	网络病毒及防范 .....	307
11.4.4	恶意代码及防范 .....	308
	思考题 .....	311
<b>第 12 章</b>	<b>黑客攻击与防范技术</b> .....	<b>312</b>
12.1	黑客基本概念 .....	312
12.1.1	什么是黑客 .....	312
12.1.2	黑客发展历史 .....	312